HPMI EXPORT CONTROL TECHNOLOGY CONTROL PLAN

SCOPE

This document describes the procedures implemented at the High-Performance Materials Institute (HPMI) for the control of technical data requiring protection from unauthorized disclosure.

AUTHORITY

The mandate for control of Technical Data at HPMI is imposed by one or more of the following:

- The United States Department of Commerce Export Administration Regulations (EAR)
- The United States Department of State International Traffic in Arms Regulations (ITAR)
- United States public law dealing with control of confidential information/ trade secrets entitled to protection from disclosure.

The Florida State University (FSU) Intellectual Property and Technology Handbook deals with controlling, protecting and transitioning to the private sector, intellectual property and technology originated by FSU staff. The emphasis of this technology control plan is to establish a means to protect applicable technical data received from other organizations while that data is at FSU for research and performance of contract activities at HPMI.

RESPONSIBILITIES

The primary responsibility of the Directors of HPMI is to maintain HPMI's integrity and stature as an academic research institution. In recognizing that the imperatives of a research institution differ from those of a corporation, the Directors will work with contracting corporations to ensure that restrictions, whether EAR- or ITAR-related, are imposed only when necessary. Appendix A provides more detailed information on specific ITAR criteria.

The Directors are responsible for implementation of this procedure. The Directors may delegate required tasks at their discretion. Clarifications or issues regarding the application and/or execution of this procedure will be referred to the Directors for resolution.

The Document Control Manager will execute this procedure and perform the day to day administrative tasks.

PROCEDURES

Acceptance of export control agreements should be kept to an absolute minimum. If “export control” language can be negotiated out of an agreement, it should be. If the project is something that we must do, we must have a plan on how to control the project specific to each case.

“Boiler plate” contracts will not be approved. Attempts should be made to designate as “fundamental research” as many tasks as possible. Only specific tasks should be designated as fundamental research. For instance, the production of Buckypaper films should remain fundamental research; however, discussions and information regarding applications should remain export control.

For each contract, the Directors shall endeavor to make the contracted work as open as possible and shall ensure that proposed control of technical data is imposed when deemed necessary.

When control measures are deemed to be necessary, PI shall recommend the Director shall determine the personnel authorized to access data for the task. The determination shall include such factors as need and status as foreign or US persons as defined by ITAR.

On a project by project basis, each authorized person shall sign a “Certification on the Handling of Controlled Data” document that acknowledges the required access and distribution restrictions for the contract. A sample briefing statement is shown in Appendix B.

The Document Control Manager shall catalog and maintain all original, signed briefing statements.

The Document Control Manager shall prepare and maintain an access list that clearly identifies the contract and the authorized personnel; the access list shall be signed by the Director with cognizance over the contract.

The Document Control Manager shall disseminate the access list to all authorized personnel on the contract, to confirm who is authorized to access data for the particular contract.

When a project or task is designated as export controlled, a file specific to that project will be established. The file will have a cover sheet clearly visible and labeled “Export Controlled.” The cover sheet will clearly list the names of personnel with access to the file. The personnel will be designated on a “need to know” basis and will meet the requirements for access to export control material. The left side of the file will have an inventory sheet listing the information contained in the file. These Export Control files will be maintained by the Operations Officer. Any file removed from the central location will be checked out, using a check out sheet that will be part of the file. Only a person named on the access list can check out the file. The check out sheet will show the printed name and signature of the person checking out the file and where the file will be located.

All export control activities will be conducted only in Room 407 of College of Engineering. If necessary, information may be removed from the building for use for attending meetings with sponsors. Information leaving the College of Engineering building must be noted on the check out sheet in the central Export Control files.

The HPMI Operations Director will be designated as the Document Control Manager.

Any manuscripts written regarding projects that are export control must be approved by the sponsor or designated activity.

RECEIPT, INVENTORY AND CONTROL OF DATA

Immediately upon receipt, all controlled data or documents shall be provided to the Document Control Manager for inventory. If it is impractical to provide the data, such as for data that exists only in an electronic form, a brief description of the data should be provided.

The Document Control Manager shall maintain an inventory of all controlled data. The inventory must include, at a minimum, the date received, the source of the data, the originator of the data, the task/contract to which the data relates, the nature of the restriction, to whom the item was released/distributed, and sufficient description to uniquely identify the item. Space should also be provided to record the date of destruction or disposition of the item from the system. (Note that "source of data" means what external organization provided the data to FSU; "Originator of data" means the organization that originally prepared the data.)

When inventorying hard copy materials, to the extent practical, the Document Control Manager will confirm each sheet of controlled data is marked to indicate its restriction. Any missing markings will be added. The Document Control Manager shall provide a conspicuous document cover sheet for each document. A sample document cover sheet is shown in Appendix C.

Electronic media (CDs, Zip Drives etc), to the extent practical, will be externally marked as well as any storage cases/ covers.

If electronic data is received via electronic means (i.e. via email or FTP), such that there is no physical media, the information provided to the Document Control Manager should be of sufficient detail that the description of the data can be recorded in the inventory.

If data is received by persons other than the Document Control Manager, the data should first be delivered to the Document Control Manager for processing.

Electronic data requiring protection, stored on computers and/or servers, must be segregated into password protected directories or network paths to assure that only those with authorized access can access the files. The Document Control Manager, in conjunction with the Network Administrator, shall ensure that the electronic access privileges are consistent with the applicable access list.

DATA CONTROL

Controlled data shall not be accessible to unauthorized persons. This includes briefings or even oral discussions that might release controlled data.

Controlled data shall not be released to third parties via reports or briefings without written authority of the originating organization.

Any duly authorized data transfers shall be performed through the Document Control Manager who will provide designation, tracking and documentation of all such transfers.

Controlled data shall not be reproduced by users. If additional copies are needed, they shall be generated and inventoried by the Document Control Manager.

Controlled data shall be under the physical control of an authorized person at all times. When not in use, data shall be in a locked container or desk; electronic files or programs should be closed so that access to them is denied to unauthorized users.

If access to controlled data is infrequent, it should be returned to the Document Control Manager for long-term secure storage.

If controlled data becomes obsolete or is no longer needed, it should be returned to the Document Control Manager for disposition. Unless otherwise directed by the terms and conditions of the specific contract, such data shall be destroyed or obliterated in such a way as to prevent reconstruction and unauthorized use, such as by shredding, disc/media destruction, file erasure etc. The Document Control Manager shall update the inventory to record the date and means of destruction, and who performed it.

Controlled data shall only be displayed or processed in areas where physical access to displays or printouts is limited to authorized persons. If it is impractical to restrict access to an entire area or lab, the operator shall assure that visitors or unauthorized persons are not permitted access to view materials.

NOTES

Section 120.10 of the ITAR provides an exemption from ITAR control for technical data which is available in the public domain through "fundamental research". Fundamental Research is defined in 120.11(a)(8) as "…basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls. University research will not be considered fundamental research if:
(i) the University or its researchers accept other restrictions on publication of scientific and technical information resulting from the project or activity, or
(ii) The research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable.

APPENDIX A

Special note: The EAR broadly covers all U.S. items, and the ITAR deals with items related to military or defense application. When technical data falls within the jurisdiction of both the EAR and the ITAR, the EAR section 734.3 (b) provides an exclusion for that item, and the ITAR alone applies. For this reason, provisions of the ITAR govern the provisions of this document.

The ITAR section 125.2(a) prohibits export of technical data to a foreign person without an export license. A foreign person is defined in 120.16 as a person who is not a lawful permanent resident of the United States of America.. Note that this definition does not apply to lawful permanent residents regardless of national citizenship.

Technical data covered by the ITAR includes:

1. Classified information relating to defense articles and defense services
2. Items that appear on, or are closely related to, the U.S. Munitions List
3. Information covered by an invention secrecy order
4. Information directly related to the design, engineering, development, production, processing, manufacture, use, operation, overhaul, repair, maintenance, modification or reconstruction of defense articles.

The U.S. Munitions List is found in section 121.1 of the ITAR. The USML consists of twenty-one categories of equipment, and category six is of particular significance to the mission of HPMI.

Category six, paragraphs (a), (f) and (g), and section 121.15 (paraphrased) result in an ITAR restriction for the following: "…technical data related to specifically designed or modified components, parts, accessories, attachments and associated equipment for warships, and any vessels specifically modified for military purposes, including vessels described as developmental, demilitarized or decommissioned.".

Section 120.10 of the ITAR provides an exemption from ITAR control for technical data which is available in the public domain through "fundamental research". Fundamental Research is defined in 120.11(a)(8) as "…basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls. University research will not be considered fundamental research if:
(i) the University or its researchers accept other restrictions on publication of scientific and technical information resulting from the project or activity, or
(ii) The research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable.

APPENDIX B

FLORIDA STATE UNIVERSITY
CERTIFICATION ON THE HANDLING OF EXPORT CONTROLLED INFORMATION

Overview: The research project identified below will involve the receipt and/or use of technical data that is controlled under United States export control laws: the Export Administration Act and Export Administration Regulations ("EAR"), enforced by the Bureau of Industry and Security in the Department of Commerce or the Arms Export Control Act and its implementing regulations, the International Traffic in Arms Regulations ("ITAR"), enforced by the Office of Defense Trade Controls in the State Department.

- **ITAR:** The ITAR control the export of equipment, technologies and technical data that are primarily military in nature. It is unlawful under the ITAR to send ITAR controlled technical data to *any* foreign persons outside the United States or to disclose – in written, oral or visual form – ITAR controlled technical data to *any* foreign persons *in* or *outside* the United States unless one of several exclusions applies or the State Department has issued a license authorizing the disclosure or export of the technical data to specific foreign persons.
- **EAR:** The EAR control the export of equipment, technologies (including software), and technical data that serve primarily civil uses. The prohibition on the export or disclosure of technical data controlled under the EAR is determined on a country-by-country basis for each disclosure of controlled technical data. As a result, it is unlawful to export technical data out of the US or to disclose technical data in or outside the US to foreign persons of countries for which a license is required as a condition of making such exports and disclosures.

Definitions:
A **"foreign person"** is anyone who is "not a lawful permanent resident" of the United States (i.e., not a green card holder) or does not have refugee or asylum status.
In general, **export controlled technical data** is specific information that is needed to develop, produce, maintain, manufacture, assemble, test, repair, operate, modify, process or otherwise use equipment or technologies that are on the control lists of the EAR or the ITAR. Controlled technical data may take the form of "blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories." Basic marketing information on function or purpose of equipment; general system descriptions; general scientific, mathematical, or engineering principles commonly taught in schools, colleges and universities and related information, and information that is in the public domain -- commonly available to interested persons – does not qualify as controlled technical data under the export control laws. The export laws and regulations determine if technical data is controlled, not your intended or actual use of the information.

Obligations: Recipients of export controlled technical data may be held personally liable for disclosures of export-controlled technical data to unauthorized foreign persons. As a result, researchers must take reasonable measures to prevent the disclosure to and use and access of export controlled technical data by unauthorized, unlicensed foreign persons. What qualifies as reasonable depends on the circumstances. Examples of measures researchers should consider adopting include clearly marking "controlled" technical data that is controlled, identifying personnel who may lawfully access the technical data, storing hard copies of

controlled technical data in locked cabinets or desks, securing access to electronic copies of and communications containing controlled technical data by passwords, user ids, or other controls; storing technical data in a single location; making only that number of copies of technical data as is necessary, and requiring all persons with lawful access to controlled technical data to sign this certification.

Penalties: Individual liability for the disclosure of controlled technical data to unauthorized foreign persons under the ITAR includes fines up to $500,000 per violation for civil violations and up to ten years imprisonment and penalties up to $1,000,000 per violation for criminal violations. Liabilities under the EAR may involve fines ranging from $10,000 to $120,000 for each civil violation and fines ranging from $50,000 to $1,000,000 for each criminal violation and 10 years imprisonment.
Individual researchers and the university also face loss of export privileges and debarment from federal contracts and grants.

Certification: I certify that I am familiar with the export control issues summarized above and have read and understand this certification. I understand that I could be held personally liable if I unlawfully disclose export controlled technical data to foreign persons and agree to take reasonable measures to prevent unauthorized foreign persons from having access to or using any export controlled technical data I may receive under the contract identified below. I agree to take appropriate security measures and to contact the FSU Office of Research- Legal Counsels Office, identified below, before making any type of disclosure of controlled technical data to any foreign person.

Signature of Researcher: _____ Date:_____

Printed Name of Researcher: _____

Department: _____

Research Project Title: _____

OMNI# _____

Sponsor: _____

Submit completed certification to Jane Mostoller Associate General Counsel. Telephone: 644-0284. Facsimile: 644-4392. Email: jmostoll@mailer.fsu.edu

For additional information on export controls, contact or visit the Bureau of Industry and Security web site at http://www.bxa.doc.gov/policiesandregulations/index.htm for information on the EAR, the Office of Defense Trade Controls web site at http://www.pmdtc.org/itar_index.htm or information on ITAR, or the FSU web site at http://www.research.fsu.edu/researchcompliance/index.html .

APPENDIX C

EXPORT CONTROLLED INFORMATION REGULATED

PI: _____DATE: _____

RETURN DATE: _____

DCM SIGNATURE: _____